UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,422	02/22/2002	Alan Rubinstein	3721.US.P	3780

56436 7590 06/19/2006

3COM CORPORATION
350 CAMPUS DRIVE
MARLBOROUGH, MA 01752-3064

EXAMINER	
PHU, SANH D	

ART UNIT	PAPER NUMBER
2618	

DATE MAILED: 06/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/082,422	RUBINSTEIN ET AL.	
	Examiner	Art Unit	
	Sanh D. Phu	2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to the RCE and Amendment filed on 4/7/06. Accordingly, claims 1-25 are currently pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spicer et al (2002/0143773), (previously cited), in view of Nakamura (6,915,422), (newly-cited).

-Regarding claim 1, see figures 1, 3, 4a and 4b, and sections [0017-0019, 0025-0064], Spicer et al discloses a method (see figure 1) comprising:

step (112) of providing wireless communication in a network (comprising (104));

step (FIREWALL) of providing a firewall protection between said network and a wireless access device (200);

step (200) of submitting an identification code (password) to said network from said wireless access device(see section [0046], wherein said identification code can be considered being associated with and pertaining to said wireless access device because said identification code is unique and sent from said wireless device (see section [0040]):

step (106) of determining the validity of said identification code (see section [0046], ;

step (110) of granting wireless network access to said wireless access device when said identification code is valid (see section [0052]);

step (110) of denying wireless network access to said wireless access device when said identification code is not valid (see section [0054]; and

step (106) of issuing an alert (a reply from a query from (110) when said identification code is not valid (see (512) of figure 4a, and sections [0052-0054]).

Spicer et al does not disclose whether the identification code (password) is a media control number, as claimed.

Using an identification number having a numerical value, as a password, for a user is well-known in the art. For instance, Nakamura teaches using an identification number having a numerical value, as a password, by selecting a combination of numerical buttons to enter the password (see col. 16, lines 8-13).

It would have been obvious for a person skilled in the art to implement Spicer et al in such a way that an identification number having a numerical value would be used as a password, as taught by Nakamura, so that the user would be able to use the wireless access device to access the network.

With such the implementation, in Spicer et al in view of Nakamura, the identification number as the password can be considered here equivalent with the limitation "a media control number".

-Regarding to claim 2, Spicer et al discloses a concentrator device (comprising (112, 114, 116, 118, 108, 110, 106) for providing said wireless communication (see figure 1) wherein said concentrator device concentrates

received signals from a plurality of wireless devices at means (112) and routes the received signals to a plurality of network resources (104) (see section [0017]).

-Regarding claim 3, Spicer et al discloses that said providing said wireless communication is accomplished in circuitry resident in said concentrator device (see figure 1).

-Regarding claim 4, as applied to claim 1, in Spicer et al in view of Nakamura, said identification number is a control number, (considered here equivalent with the limitation "media access control number"), of said wireless device so that the user would be able to use the wireless access device to access the network.

-Regarding claim 5, Spicer et al discloses that said determining said validity of said identification code is accomplished by reference to a list of valid identification codes (see section [0031]).

-Regarding claim 6, Spicer et al discloses a concentrator device comprises (112, 114, 116, 118, 108, 110, 106) (see figure 1) wherein means

(106) in said concentrator device stores said list of valid identification codes (see section [0031]).

-Regarding claim 7, Spicer et al discloses that said list of valid identification codes is resident in a server (106) in said network (see figure 1).

-Regarding claim 9, Spicer et al discloses that said network is a wireless personal area network (local area network) (see sections [0022, 0018].

-Regarding claim 10, see figures 1, 3, 4a and 4b, and sections [0017-0019, 0025-0064], as similarly applied to claim 1, Spicer et al discloses a system (see figure 1) comprising:

a server (106);

a wireless connection device (112) communicatively coupled with said server;

a wireless access device (200) enabled to wirelessly submit an identification code (password) to said wireless connection device, said identification code associated with and pertaining to said wireless access device; and

a firewall(110, FIREWALL)communicatively coupled to said server and said wireless connection device,

wherein said firewall is enabled to grant network access to said wireless access device when said identification code is valid and to deny access to said network by said wireless access device and issue an alert when said identification code is not valid.

Spicer et al does not disclose whether the identification code (password) is a media control number, as claimed.

Using an identification number having a numerical value, as a password, for a user is well-known in the art. For instance, Nakamura teaches using an identification number having a numerical value, as a password, by selecting a combination of numerical buttons to enter the password (see col. 16, lines 8-13).

It would have been obvious for a person skilled in the art to implement Spicer et al in such a way that an identification number having a numerical value would be used as a password, as taught by Nakamura, so that the user would be able to use the wireless access device to access the network.

With such the implementation, in Spicer et al in view of Nakamura, the identification number as the password can be considered here equivalent with the limitation "a media control number" .

-Regarding claim 11, Spicer et al discloses that said server is an internet portal (see section [0018]).

-Regarding claim 12, as similarly applied to claim 2, Spicer et al discloses that connection device is an concentrator device enabled for wireless communication (see figure 1).

-Regarding claims 13-16, Spicer et al discloses that said wireless access device is a wirelessly enabled laptop computer, computer peripheral device, personal data assistant or wireless telephone (see section [0019]).

-Claim 17 is rejected with similar reasons set forth for claim 2.

-Regarding claim 18, Spicer et al discloses that said firewall is enabled to obtain a list of valid identification codes from said server (see section [0031]).

-Regarding claim 19, Spicer et al discloses that firewall is enabled to verity the validity of said identification code submitted from a wireless access device (see sections [0052-0054]).

-Regarding claim 8, Spicer et al in view of Nakamura does not disclose that said denying said wireless access to said network is accomplished simultaneously with granting access to said wireless accesses devices with valid identification codes.

However, the examiner takes Official Notice using multiple access schemes, e.g., TDMA, CDMA, FDMA, etc., for simultaneously receiving, processing and/or responding a plural of received signals each sent from a different remote station is well-known in the art.

Therefore, it would have been obvious for a person skilled in the art to implement Spicer et al with a multiple access scheme in such a way that Spicer et al invention would be capable of simultaneously receiving of access requests from a plurality of wireless accesses devices and simultaneously responding by denying a wireless access to said network to a wireless access device with invalid identification code and granting access to wireless accesses devices with valid identification codes so that Spicer et al invention would be capable of operating in a high speed for promptly responding to access requests from said wireless accesses devices.

-Regarding claim 20, see figures 1, 3, 4a and 4b, and sections [0017-0019, 0025-0064], Spicer et al discloses a concentrator device (see figure 1), comprising:

a housing (enterprise)(see section [0023];

electronic circuitry (112, 110, 114, FIREWALL) enabled to wirelessly communicate with a wireless access device (200) and a network (116, 118, 104); and

a distributed firewall (110, 114, FIREWALL) resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device, said control via a valid identification code (password) associated with and pertaining to said wireless access device, said identification code being transmitted from said wireless access device.

Spicer et al does not disclose a cable connector coupled to said housing and adapted to communicatively couple said concentrator device to a network data cable.

Using a cable (equivalent with "network data cable") to couple between two networks, the cable onto which a communication between the two networks is provided, is well-known in the art, and the examiner takes Official Notice.

It would have been obvious for a person skilled in the art to implement Spicer et al by using a cable to connect means (FIREWALL) of said concentrator device with means (116) of the network (116, 118, 104) in order to enable the required communication between the wireless access device (200) and the network (116, 118, 104).

In such an implementation, a cable connector is inherently included in Spicer et al in order to connect means (FIREWALL) with the cable.

Further, since means (FIREWALL)of said concentrator device is located on the housing (enterprise)(see section [0024], with such the implementation, it can be said that the cable connector is coupled to said housing and adapted to communicatively couple said concentrator device to the cable.

Spicer et al does not disclose whether the identification code (password) is a media control number, as claimed.

Using an identification number having a numerical value, as a password, for a user is well-known in the art. For instance, Nakamura teaches using an identification number having a numerical value, as a password, by selecting a combination of numerical buttons to enter the password (see col. 16, lines 8-13).

It would have been obvious for a person skilled in the art to implement Spicer et al in such a way that an identification number having a numerical value would be used as a password, as taught by Nakamura, so that the user would be able to use the wireless access device to access the network.

With such the implementation, in Spicer et al in view of Nakamura, the identification number as the password can be considered here equivalent with the limitation "a media control number".

-Regarding claim 21, Spicer et al does not disclose that said concentrator device comprises a hub.

The Examiner takes Official Notice that using a wireless hub to enable a wireless communication between a remote station and a network is well-known in the art.

Therefore, it would have been obvious for a person skilled in the art to implement Spicer et al concentrator device with a wireless hub for wirelessly receiving/transmitting signals from/to the wireless access device (200) in order to enable the required wireless communication between the wireless access device (200) and network (116, 118, 104).

-Regarding claim 22, as similarly applied to claim 7, Spicer et al discloses that said distributed firewall is enabled to obtain a list of valid identification codes from a server (106) (see figure 1).

-Regarding claim 23, as similarly applied to claim 1, Spicer et al in view of Nakamura discloses that said distributed firewall is enabled to verify validity of said identification code submitted by a wireless access device, said identification code being a number (considered here equivalent with the limitation "media access control number").

-Regarding claim 24, as similarly applied to claim 1, Spicer et al discloses that said distributed firewall is enabled to deny access to said wireless access device if said identification code is not valid.

-Regarding claim 25, as similarly applied to claim 1, 3 discloses that said distributed firewall is enabled to issue an alarm to a network manager (110) is said identification code is not valid (see figure 1).

Response to Arguments

4. Applicant's arguments filed on 4/27/06 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sanh D. Phu whose telephone number is (571)272-7857. The examiner can normally be reached on M-Th from 7:00-17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matthew D. Anderson can be reached on (571) 272-4177. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sanh D. Phu
Examiner
Division 2618

6/13/06

SP

SANH D. PHU
PATENT EXAMINER